

AN15173

Identifying MCX E31/E32 Devices and Inspecting HSE-B Firmware with J-Link Commander

Rev. 1.0 — 22 September 2026

Application note

Document information

Information	Content
Keywords	MCX E31, MCX E32, HSE-B, J-Link Commander, MIDR1, Messaging Unit, GET_ATTR, FullMem
Abstract	This application note describes a J-Link Commander-based utility that identifies supported MCX E31 and MCX E32 devices without a target application, reports SBAF and HSE-B status, issues a read-only HSE_SRV_ID_GET_ATTR request through MU0 channel 1, and provides an explicitly confirmed FullMem HSE-B installation flow for authorized laboratory boards.



1 Introduction

During the initial board inspection, a customer or field application engineer must often identify the device, confirm the HSE-B initialization, and read the SBAF and HSE-B firmware versions. Building a target application only for these checks adds to setup time and can introduce a device-selection error.

The MCXE3_HSE_JLink_Demo package performs these checks from Windows PowerShell through J-Link Commander and SWD. It connects with the generic Cortex-M7 profile, reads the device identity, selects package mapping, and issues a read-only HSE-B service request. No target application image is required.

1.1 Scope

The supplied device table covers MCX E315, MCX E316, MCX E317, MCX E31B, MCX E327, and MCX E32B. The utility reads the identification and status information, writes a temporary descriptor and result buffer in SRAM, and requests the firmware-version attribute through MU0 channel 1. A separate installer can place a matching FullMem image on an authorized blank or erasable laboratory board.

This application note focuses on J-Link-based inspection and laboratory installation. For HSE-B concepts, Secure Boot, key handling, life cycle configuration, SEC Tool, Flashloader, and provisioning workflows, see *Getting Started with HSE-B Security Module on MCX E31/E32* ([AN15120](#)) [1].

2 Software package and supported devices

This chapter describes the software package and supported devices.

2.1 Utility entry points

The package exposes two user-facing command launchers:

- The `run_hse_live_check.cmd` file identifies the device and reports the SBAF and HSE-B information. It does not intentionally modify the persistent target storage.
- The `install_hse_fullmem.cmd` file performs a guarded FullMem installation after automatic identification, package-integrity checking, and exact operator confirmation.

The `hse_live_check.ps1` PowerShell entry point returns without pausing for scripted use. The command launcher pauses only to keep the console visible.

2.2 Supported-device mapping

Table 1. Predefined MCXE3 device mappings

MIDR1 part	Device	FullMem image	J-Link profile
0x136	MCXE315	mcxe315_hse_fw_0.12.0_2.55.0_pb250324.bin	MCXE315
0x137	MCXE316	mcxe316_hse_fw_0.12.0_2.55.0_pb250324.bin	MCXE316
0x138	MCXE317	mcxe317_hse_fw_0.13.0_2.55.0_pb250324.bin	MCXE317
0x13A	MCXE31B	mcxe31b_hse_fw_0.5.0_2.55.0_pb250324.bin	MCXE31B
0x142	MCXE327	mcxe317_hse_fw_0.13.0_2.55.0_pb250324.bin	MCXE317
0x144	MCXE32B	mcxe31b_hse_fw_0.5.0_2.55.0_pb250324.bin	MCXE31B

MCX E327 reuses the MCX E317 FullMem image and J-Link profile. MCX E32B uses the MCX E3xB image represented by the MCX E31B file and selects the MCX E31B profile.

The method is not tied to MCX E317. It also applies to MCX E devices that provide the same SIUL2 identification, SBAF status source, and MU/HSE-B host interface. Adding a device requires its MIDR1 part code, matching FullMem image, and J-Link programming profile.

3 Hardware and software prerequisites

- Windows PowerShell 5.1 or later.
- J-Link Commander 9.32 or later. If several installations are present, the utility parses their directory versions and selects the highest supported version.
- A J-Link debug probe connected to the target SWD signals, including the reset signal where required by the board connection.
- A powered development board, blank board, or other laboratory board for which debug access and any requested erase operation are authorized.
- All other SEGGER and debug sessions closed before the utility starts.
- The complete software package, including the firmware directory, when the FullMem installation path is used.

CAUTION: *The inspection path is not nonintrusive. It writes the volatile SRAM, uses an MU channel, and J-Link can halt or reset the core and initialize the ECC-protected RAM when connecting to MCX E31 devices [6]. Do not use this workflow on a running production system or when a runtime state must be preserved.*

[Figure 1](#) shows a laboratory run on an FRDM-MCXE31B board reworked with an MCX E317 device. It illustrates the expected SBAF, HSE-B, and GET_ATTR output. The device-table-driven procedure is not specific to MCX E317.

4 Device identification and status sources

This chapter describes the device identification and status sources.

4.1 Device identification from SIUL2.MIDR1

The bootstrap J-Link session selects CORTEX-M7 and reads SIUL2.MIDR1 at 0x40290004. The fields are defined in the *MCX E31x Reference Manual* ([MCXE31XRM](#)), section 9.6.2, MIDR1 [2].

- MIDR1[31:26]: product-line code
- MIDR1[25:16]: part-number code
- MIDR1[7:4]: major mask revision
- MIDR1[3:0]: minor mask revision

For example, a raw value of 0x2D380000 gives product-line code 0x0B, part-number code 0x138, major mask 0, and minor mask 0. [Table 1](#) maps part code 0x138 to MCX E317. The mask revision is reported as information and is not compared with a fixed acceptance value.

4.2 SBAF identity and version field

The utility reads the 64-bit SBAF version field at 0x4039C020, described in the *HSE-B Firmware Reference Manual* ([HSEFWRM](#)), section 14.6.4.1, Secure BAF version [3]. Word 0 supplies the SoC ID from bits [15:8] and firmware type from bits [31:16]. Word 1 is displayed in the reserved.baseline.incremental.RC order.

In [Figure 1](#), raw words 0x00000D00 and 0x06000F00 decode to SoC ID 13, standard firmware, and version 0.15.0.6. The version is reported but it is not a PASS criterion.

4.3 HSE initialization status from MU0_MUB.FSR

The utility reads MU0_MUB.FSR at 0x4038C104 and sends the service request only when bit 24, HSE_STATUS_INIT_OK, is set. See the *MCX E31x Reference Manual* ([MCXE31XRM](#)), section 39.7.1.1 [2], and the *HSE-B Firmware Reference Manual* ([HSEFWRM](#)), section 2.5.1.3 [3].

4.4 Keeping reported identifiers separate

Table 2. Sources of identification and status data

Reported item	Source	Meaning in the utility
Device, part code, mask	SIUL2.MIDR1 at 0x40290004	Selects one of the six device profiles and reports the silicon mask fields.
SBAF SoC ID, type, version	64-bit field at 0x4039C020	Reports the SBAF identity and four-byte version representation.
HSE initialized	MU0_MUB.FSR at 0x4038C104, bit 24	Gates the live HSE-B service request.
Memory configuration, HSE SoC ID, type, version	HSE_FW_VERSION_ATTR_ID returned by GET_ATTR	Reports HSE-B data returned by the running firmware.

The MIDR1 part-number code, SBAF SoC ID, and HSE firmware SoC ID originate from different structures. They must not be treated as interchangeable identifiers. Device selection is based only on the MIDR1 part-number field.

5 Live HSE-B service check

This chapter describes the live HSE-B service check.

5.1 GET_ATTR service descriptor

After confirming HSE_STATUS_INIT_OK, the utility writes a service descriptor at 0x20400000 and clears the 8-byte output buffer at 0x20400100. These volatile SRAM writes request HSE_FW_VERSION_ATTR_ID through HSE_SRV_ID_GET_ATTR [4].

Table 3. GET_ATTR descriptor written at 0x20400000

Offset	Value	Purpose
0x00	0x00A50002	HSE_SRV_ID_GET_ATTR service ID
0x04	0x00000000	Metadata/reserved field
0x08	0x00000001	Attribute ID 1, HSE_FW_VERSION_ATTR_ID
0x0C	0x00000008	Output length, 8 bytes
0x10	0x20400100	Output-buffer pointer

5.2 MU0 channel 1 request and response

The host-to-HSE path uses MU0 channel 1. The utility proceeds when TSR bit 1 indicates that TR1 can accept a request and RSR bit 1 is clear. This is a transmit/receive precheck rather than a broader MU ownership check.

- TSR at 0x4038C124: bit 1 must indicate that the channel 1 transmit register can accept a request.
- RSR at 0x4038C12C: bit 1 must be clear before the transmission and set when the response is ready.

- TR1 at 0x4038C204: receives the descriptor address 0x20400000.
- RR1 at 0x4038C284: provides the HSE service response code.

The relevant MU instances and register maps are described in the *MCX E31x Reference Manual* ([MCXE31XRM](#)), sections 39.1.1 and 39.7.1.1. TR1 and RR1 are described in sections 39.7.1.17 and 39.7.1.18 [2]. The MU and request protocol are described in the *HSE-B Firmware Reference Manual* ([HSEFWRM](#)), sections 2.5.1 and 2.5.1.3 [3].

5.3 PASS meaning and ABSwap handling

HSE FUNCTIONAL RESULT: PASS has a deliberately narrow meaning. It indicates all of the following:

- The MIDR1 part-number field matched one of the six package profiles.
- HSE_STATUS_INIT_OK was set in MU0_MUB.FSR.
- The TSR/RSR transmit/receive precheck for channel 1 passed.
- The response-ready bit was set after the fixed wait, RR1 contained 0x55A5AA33, and the firmware-version attribute payload was readable.

The 0x55A5AA33 value is the HSE service success response. The SBAF version, HSE-B version, mask revision, and memory configuration are informational and are not compared with fixed expected values. A running ABSwap configuration can therefore pass the live check. The separate installer supports FullMem only and does not convert or overwrite an initialized ABSwap installation.

6 Running the utility

This chapter describes how to run the utility.

6.1 Run the live check

1. Install J-Link Commander 9.32 or later. The package does not install or update the SEGGER tools.
2. Power the authorized development or laboratory board and connect the J-Link probe through SWD.
3. Close J-Link Commander, J-Flash, J-Link GDB Server, RTT Viewer, IDE debug sessions, and other applications that own the probe.
4. Run the `run_hse_live_check.cmd` file. For automation, invoke the `hse_live_check.ps1` file directly with an appropriate PowerShell execution policy.
5. Review the Device, MIDR1, mask, SBAF information, HSE status, memory configuration, firmware version, GET_ATTR response, and the final result.

```
.\run_hse_live_check.cmd
powershell.exe -NoLogo -NoProfile -ExecutionPolicy Bypass -File .
\hse_live_check.ps1
```

A successful run returns exit code 0. An unrecognized device, missing tool, unsupported J-Link version, busy request path, uninitialized HSE-B firmware, missing response, or service error return a nonzero exit code with one primary reason.

6.2 Failure indications

Table 4. Common failure indications

Indication	Meaning and next check
J-Link Commander was not found/9.32 or newer is required	Install a supported J-Link package or remove the ambiguity between installations. Rerun it after closing all SEGGER sessions.

Identifying MCX E31/E32 Devices and Inspecting HSE-B Firmware with J-Link Commander

Table 4. Common failure indications...continued

Indication	Meaning and next check
Unsupported MCX E3 part-number code	The value read from MIDR1[25:16] is not in the six-device table. Confirm the target power, SWD integrity, and the actual device.
HSE is not initialized	The MU0_MUB.FSR bit 24 is clear. Confirm whether the HSE-B is expected on this board before considering installation.
MU0 channel 1 is busy	The TSR bit 1 was cleared or the RSR bit 1 already contained a response. Close the software that may use the MU and return the board to an idle laboratory state.
HSE response was not ready	The RSR bit 1 was still clear after the single 500-ms period. Reset or power-cycle the laboratory board and repeat it. Persistent failures require the HSE-B diagnosis.
GET_ATTR failed with response 0x.	RR1 returned an HSE error rather than 0x55A5AA33. Record the response and interpret it with the <i>HSE-B Firmware Reference Manual</i> (HSEFWRM).
J-Link failed during device detection/service request	The external command failed or its expected memory output was absent. Review the J-Link console connection result.

6.3 MCX E317 laboratory example

[Figure 1](#) shows a representative run on an FRDM-MCX E31B board reworked with an MCX E317 device. The crop preserves the original SBAF, HSE-B, GET_ATTR, and result values.

```

SBAF
Raw          : 0x00000D00 0x00000F00
SoC ID       : 13
Firmware type : Standard
Version      : 0.15.0.6

HSE firmware
FSR raw      : 0x09600000
HSE_STATUS_INIT_OK : YES
Memory configuration : FullMem
SoC ID       : 13
Firmware type : Standard
Version      : 2.55.0
GET_ATTR response : 0x55A5AA33 (OK)

OVERALL RESULT: PASS

```

Figure 1. HSE-B status and GET_ATTR response on a reworked FRDM-MCX E31B fitted with an MCX E317 device

The same fields are reported for each mapped device. The MIDR1, mask, SBAF version, HSE-B version, and memory configuration vary with the device and installed firmware.

7 Guarded FullMem HSE-B installation

This chapter describes how to install the Guarded FullMem HSE-B.

7.1 Installation controls

The persistent installation path is separate from the live check. Run the `install_hse_fullmem.cmd` file only on a board for which erasing the listed program-flash range and writing the HSE usage flag are explicitly allowed. The script repeats automatic MIDR1 identification and does not offer a manual device override.

If HSE_STATUS_INIT_OK is already set, the installer stops. Otherwise, it selects the mapped firmware and J-Link profile, checks the packaged image, and displays the device, image, erase range, and UTEST write before asking for confirmation.

Identifying MCX E31/E32 Devices and Inspecting HSE-B Firmware with J-Link Commander

The confirmation is case-sensitive and must exactly match `INSTALL <device>`, where `<device>` is the automatically identified name, for example:

```
INSTALL MCXE317
```

After confirmation, J-Link erases `0x00400000-0x0043FFFF`, loads and verifies the FullMem image at `0x00400000`, writes the 64-bit HSE usage flag `0xAABBCCDDDDCCBBAA` at UTEST address `0x1B000000`, reads it back, resets the target, and runs the live check.

CAUTION: *The FullMem installation is a laboratory operation for an authorized development or blank board. It is not a production provisioning procedure. See [Getting Started with HSE-B Security Module on MCX E31/E32 \(AN15120\)](#) and the approved NXP provisioning tools for Secure Boot, key management, life cycle configuration, and production deployment [1].*

8 Applicability to other MCX E devices

This chapter describes the applicability to other MCX E devices.

8.1 Common mechanism

The device identification, SBAF decoding, MU request, and GET_ATTR processing use common SIUL2 and HSE-B interface mechanisms. MCX E317 is the example in this document, not a special execution path.

For a device with the same host interface, the live-check sequence remains unchanged. Only device-specific mapping data and the displayed values differ.

8.2 Extending the device table

To add an MCX E device, define its MIDR1 part code, device name, matching FullMem image, and J-Link programming profile. Confirm the device memory and UTEST conventions in the applicable reference documentation.

8.3 Scope boundaries

- The utility covers the HSE-B inspection and guarded FullMem installation on development or laboratory hardware.
- It does not configure Secure Boot, keys, life cycle, or production provisioning. See *Getting Started with HSE-B Security Module on MCX E31/E32* ([AN15120](#)) for those workflows.
- The supplied table contains six MCX E3 mappings. Other MCX E devices can be added through the mapping data described above.

9 Acronyms

Table 5. Acronyms and abbreviations

Term	Meaning
API	Application Programming Interface
ECC	Error Correcting Code
FAE	Field Application Engineer
FRDM	Freedom Development Platform
FSR	Flag Status Register

Table 5. Acronyms and abbreviations...continued

Term	Meaning
HSE-B	Hardware Security Engine, B configuration
IDE	Integrated Development Environment
MIDR1	MCU Identification Register 1
MU	Messaging Unit
RC	Release Candidate
RTT	Real-Time Transfer
SBAF	Secure Boot Assist Flash
SDK	Software Development Kit
SEC Tool	Secure Provisioning Tool
SoC	System on Chip
SRAM	Static Random-Access Memory
SWD	Serial Wire Debug
TSR	Transmit Status Register
UTEST	User Test/one-time-programmable memory region

10 References

- [1] NXP Semiconductors, [AN15120](#), *Getting Started with HSE-B Security Module on MCX E31/E32*
- [2] NXP Semiconductors, *MCX E31x Reference Manual*: section 9.6.2, MIDR1; section 39.1.1, MU instances; section 39.7.1.1, MU0_MUB memory map; sections 39.7.1.17 and 39.7.1.18, TR1 and RR1.
- [3] NXP Semiconductors, *HSE-B Firmware Reference Manual*: section 2.4.2.4.2, Usage; section 2.5.1, Messaging Unit; section 2.5.1.3, HSE status; section 14.6.4.1, Secure BAF version.
- [4] NXP Semiconductors, *HSE Service API Reference Manual*: Host Interface, GET_ATTR and service response; Administration Services, hseGetAttrSrv_t, hseAttrFwVersion_t, and HSE_FW_VERSION_ATTR_ID.
- [5] NXP Semiconductors, MCUXpresso SDK ELE_HSEB firmware README.
- [6] SEGGER Microcontroller GmbH, NXP MCX E31 Knowledge Base, https://kb.segger.com/NXP_MCX_E31.

11 Revision history

Table 6. Revision history

Document ID	Release date	Description
AN15173 v.1.0	22 September 2026	Initial release

Legal information

Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at <https://www.nxp.com/profile/terms>, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Suitability for use in non-automotive qualified products — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

HTML publications — An HTML version, if available, of this document is provided as a courtesy. Definitive information is contained in the applicable document in PDF format. If there is a discrepancy between the HTML document and the PDF document, the PDF document has priority.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately. Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

Identifying MCX E31/E32 Devices and Inspecting HSE-B Firmware with J-Link Commander

AMBA, Arm, Arm7, Arm7TDMI, Arm9, Arm11, Artisan, big.LITTLE, Cordio, CoreLink, CoreSight, Cortex, DesignStart, DynamIQ, Jazelle, Keil, Mali, Mbed, Mbed Enabled, NEON, POP, RealView, SecurCore, Socrates, Thumb, TrustZone, ULINK, ULINK2, ULINK-ME, ULINK-PLUS, ULINKpro, μ Vision, Versatile — are trademarks and/or registered trademarks of Arm Limited (or its subsidiaries or affiliates) in the US and/or elsewhere. The related technology may be protected by any or all of patents, copyrights, designs and trade secrets. All rights reserved.

J-Link — is a trademark of SEGGER Microcontroller GmbH.

Contents

1	Introduction	2
1.1	Scope	2
2	Software package and supported devices	2
2.1	Utility entry points	2
2.2	Supported-device mapping	2
3	Hardware and software prerequisites	3
4	Device identification and status sources	3
4.1	Device identification from SIUL2.MIDR1	3
4.2	SBAF identity and version field	3
4.3	HSE initialization status from MU0_	
	MUB.FSR	4
4.4	Keeping reported identifiers separate	4
5	Live HSE-B service check	4
5.1	GET_ATTR service descriptor	4
5.2	MU0 channel 1 request and response	4
5.3	PASS meaning and ABSwap handling	5
6	Running the utility	5
6.1	Run the live check	5
6.2	Failure indications	5
6.3	MCX E317 laboratory example	6
7	Guarded FullMem HSE-B installation	6
7.1	Installation controls	6
8	Applicability to other MCX E devices	7
8.1	Common mechanism	7
8.2	Extending the device table	7
8.3	Scope boundaries	7
9	Acronyms	7
10	References	8
11	Revision history	8
	Legal information	9

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.
